Denver Health
HIPAA Privacy Assessment

Federal Register Vol.64, No 212, pgs. 59918-60065

The proposed privacy rules:

- Define and limit the circumstances in which covered entities may use and disclose covered health information
- Establish individual rights with respect to the covered health information
- Require covered entities to adopt safeguard to protect the confidentiality of covered health information and protect against unauthorized access

Protected Health Information: Information that relates to an individual's health, health care treatment, or payment for health care and that identifies the individual.

State Laws

- All HIPAA Privacy rules are preempted by more stringent existing state privacy laws

Assessment – Review of state law related to privacy of health information and patient rights related to health information

Uses and Disclosures of PHI without Individual Authorization

- Permissive Disclosure §164.506 (a)(1). A covered entity is permitted to use or disclose PHI without individual authorization:
  - ◊ Information may released without specific individual consent to carry out treatment, payment or health care operations
  - ◊ For certain national priority purposes (such as research, public health and oversight, (see Attachment A) but only under defined circumstances
- Mandatory Disclosures §164.506 (a)(2). A covered entity is required to disclose PHI without individual authorization:
  - ◊ In response to a request by an individual to inspect, and obtain a copy of, his PHI
  - ◊ In connection with an enforcement action or compliance review brought by the Secretary of HHS

Assessment: Review current policies, practices and documents related to release of or reporting PHI.

Uses and Disclosures of PHI with Individual Authorization

Authorization Requested by Individuals (Patients)

The individual (patient) requesting a use or disclosure must submit an authorization form to the covered entity.

The form must:

- Provide a specific description of the information to be used or disclosed
- Name the covered entity authorized to make the requested use or disclosure
- Name the party to whom the covered entity may make the request use of disclosure
- Provide an expiration date
- Be sign and dated
- Be in plain language (Note – the rule has a "model" form that can be used or adapted.)

Assessment – Review current policy and authorization forms for patient request for record release including process to verify the individual's

identity.

Authorizations Requested by Covered Entities

A covered entity requesting use or disclosure must obtain an authorization from the subject of the information

The form used must:

- Provide a specific description of the information to be used or disclosed
- Name the covered entity authorized to make the requested use or disclosure
- Name the party to whom the covered entity may make the request use of disclosure
- Include statements concerning
  a) the purpose for which the request was made
  b) the right of the individual to inspect or copy information
  c) the right of the individual to refuse treatment
  d) whether authorization will result in financial gain for the covered entity
- Provide an expiration date
- Be sign and dated

Covered entities must also have procedures in place to limit the scope of the request to the minimum amount of information needed to achieve the purpose for which the information is requested.

Assessment: Review the organization's policy and forms used to request information from other covered entities. Review the organization's policy and process to release records to requesting entities including patient authorization and verification of identify or authority of requesting entity.

Note: Authorizations to release information requested by individuals or by covered entities can be time or date limited and are revocable at any time.

Covered entities can meet the privacy standards by removing specified identifying data elements that might identify the individual. These data elements include: (pg. 59936)

- Name
- Address, including street address, city, country, zip code
- Names of relatives and employers
- Birth date
- Telephone and fax numbers
- e-mail address
- Social Security number
- Medical Record number
- Health plan beneficiary number
- Account number
- Certificate/License number
- Any vehicle or other device serial number
- Web URL
- Internet Protocol (IP) Address
- Finger or voice prints
- Photographic images
- Any other unique identifying number characteristic, or code

Individual Rights

REQUIREMENT	IMPLEMENTATION	ASSESSMENT
Right to receive written notice of the covered entities information practices	See Administrative Requirements	
Individual Requested Restrictions to Access Restriction of disclosure or use for healthcare treatment, payment or health care operations – pertains only to providers	Assess feasibility of limiting use and disclosure Document how covered entities would implement an individual's request to restrict uses and disclosures. (59993)	System function to control access to specific patient records by named individuals or groups of individuals Policy related to limited record access
Individual Request to Inspect and Copy PHI The rule uses a designated record set concept. The set is a group of any records under the control of any covered entity from which information is retrieved by the name of the individual or by some identifying number, symbol or other identifying particular assigned to the individual. See page 59933 for further detail.	Process must be in place for individuals to request to review their PHI, to review their PHI, and to obtain a copy of their PHI. Process to access information maintained by business partners when that information is different than that maintained by the covered entity. Limited grounds for denial of access to PHI – see pages 59982-83 See pg. 59984 for Time limits, accepted or denied requests and copy fees	Existing P&Ps for: ❑ Patient access to review their PHI ❑ Patient receipt of/or copying their PHI Check patient rights related to Medicare/ Medicaid regulations
Individual Request to correct or Amend PHI	Process must be in place for individual's to request an amendment to or correction of PHI. Provider or plan required to accommodate request with respect to any information that the plan or providers determines to be erroneous or incomplete, that was created by the plan or provider. See 59986-59988 for processes to determine if information should be amended, timeframes, denials, and inclusion in original record.	Existing P&Ps for: ❑ Patient access to review their PHI ❑ Patient modification of the PHI
Individual right to receive an accounting of how their protected health information has been disclosed. *Disclosure*: This term would be defined as the	Individuals have a right to receive an accounting of all instances where PHI is *disclosed* by a covered entity for purposes other than treatment, payment, and health care operations.	Current process of logging when information is released or disclosed and for what purposes. System's audit capabilities to track

release, transfer, provision of access to, or divulging in any other manner of information **outside the entity holding the information**.	The rules do not specify the form of the accounting, but would include: ▪ the date of disclosure ▪ the name and address of the organization or person who received the PHI ▪ a brief description of the information disclosed. Accounting of disclosures, including copies of signed authorization forms, be made available as quickly as possible, but not later than 30 days following receipt of the request	release of PHI

Administrative Requirements: In order to protect identifiable health information from inappropriate access, use or disclosure, covered entities are required to develop and implement basic administrative procedures to protect the confidentiality of health information and the right of individuals and to maintain documentation of the P&Ps used by covered entities to comply with the requirements.

Designation of a Privacy Official	Designate a privacy official responsible for the development and implementation of privacy related policies and procedures	
Establish Training Programs for Employees	Provide training on the organization's P&PS related to protected health information. Each organization would provide training at the time the rule becomes applicable, for each new employee, and when a change is made in the P&Ps Training is required for all employees, volunteers, trainees, and other persons who are likely to have contact with protected health information At least one every 3 years employees would sign a new statement certifying that he or she will honor all of the entity's privacy policies.	Current training related to privacy and/or confidentiality of patient information. Documents related to employee honoring privacy or confidentiality policies.
Implement safeguards to protect health information from intentional or accidental misuses	Require covered entities to put in place administrative, technical, and physical safeguards to protect against any reasonably anticipated threats or hazards to the privacy of the information, and unauthorized uses or disclosures of the information. (See also Security rules) Administrative would include verification procedures for release of information and protection for whistleblowers	
Develop a system for individuals to lodge complaints about an entity's information practices	Maintain a process for receiving complaints regarding the covered entity's compliance to the privacy rule and for maintaining a record of complaints filed.	Existing P&Ps for ❑ Complaints about inappropriate or unauthorized record access ❑ Denial of access to records ❑ Process for record keeping of any complaints received.
Sanctions	Develop and apply when appropriate sanctions for failure to comply with P&Ps of the covered entity or with the requirements of this proposed rule	Review: : ❑ Existing ES&R or CSA policies

	or with the requirements of this proposed rule.	related to Violation of pt privacy/confidentiality and related sanctions ❑ Vendor/business partner contracts related to breeches of confidentiality and sanctions
Duty to Mitigate	Covered entities have procedures for mitigating, to the extent practicable, any deleterious effect of a use or disclosure of PHI by their member of their workforce or business partners.	
Development and Documentation of Policies and Procedures	Develop and document P&PS for implementing the requirements of the rule. ❑ Uses and Disclosures of PHI ❑ Individual Requests for Restricting Uses and Disclosures ❑ Notice of Information Practices ❑ Inspection and Copying ❑ Amendment or Correction ❑ Accounting for Disclosures ❑ Administrative Requirements ❑ Record Keeping Requirements	Existing P&Ps related to required rule components.
Processes to limit access to PHI to only the information an employee or subset of employees need in the course of their work	A central aspect of the Privacy rules is the principle of "minimum necessary" disclosure. With certain exceptions, permitted uses and disclosures of PHI would be restricted to the minimum amount of information necessary to accomplish the purpose for which the information is used, taking into consideration practical and technological limitations.	Current process to determine what systems/ information an employee or group of employees needs in the course of their work Processes to limit system access or access within a system to the defined required information.

Notice of Information Practices

See example language pg. 60049

The notice is required to include:

- An explanation of the way the entity uses and discloses protected health information
- Basic statements relating to individual's rights (as outlined in the rule, see previous Individual Rights section)
- Identification of a contact person for complaints and additional information
- The date of the notice.

- ❑ Patient rights documents
- ❑ Policies related to disclosure of information
- ❑ Policies related to release of information

The Privacy rules extend to those who do business with the defined covered entities through Business Partner Agreements

Note: The Coding and Transaction Standards rule will require a "Chain of Trust" agreement between organizations exchanging data electronically.

The Business Partner Agreement (BPA) is designed for business partners of covered entities that have access to patient information whether or not in EDI form (e.g. software vendors, consultants, collection agencies, billing services, utilization review outsourcing, etc.).

The Privacy NPRM specifically excludes BPA's with physicians sharing patient information for the purpose of treatment.

Eleven Required Contractual Provisions §164.506 (e)(2)(i)

Identify Business partners

- ❑ Vendors
- ❑ Consultants
- ❑ Service Providers
- ❑ Other

Research

Research is defined as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge (From the Federal Policy for the Protection of Human Subjects aka "the Common Rule")

Review

- ❑ Current IRB processes
- ❑ Current research review not covered by IRB including record review
- ❑ Current HIM research related record release processes
- ❑ Current patient authorizations to be included in research cohorts

- Documentation of Compliance Monitoring including Business Partners

Security training awareness required for all employees, agents, and contractors.
Training based on job responsibilities

Uses and Disclosure Permitted without Individual Authorization (pgs. 59955 – 59976) § 164.510(b) – 164.510(m)

Attachment A

PHI can be disclosed for purposes other than treatment, payment, and health care operations without individual authorization for certain purposes and under specific conditions. For some purposes individual permission is still required, but it is informal verbal agreement vs. a written authorization.

Purpose	Conditions
Public Health Activities pg. 59955	
Public health activities include the prevention or control of disease, injury or disability, reporting would include diseases, injuries and conditions, reporting of vital events such as birth and death, public health activities undertaken by the FDA (AMI and device reporting)	Disclosure to 3 types of authorities: ▪ public health authorities, ▪ non-governmental entities authorized by law to carry out public health activities, ▪ persons who may be at risk of contracting or spreading a disease. Covered entities would have to verify the identity of persons requesting PHI and the legal authority supporting that request before disclosure is permitted. This rule does not preempt state law regarding "public health surveillance, or public health investigation or intervention"
Health Oversight Activities pg. 59957	
PHI can be disclosed to public oversight agencies and to private entities acting on behalf of such agencies without individual authorization, for health oversight activities authorized by law. See also the definition of Health Care Operations, pgs 59933-34 for organizations or activities to which PHI can be disclosed.	Covered entities could disclose PHI to a health oversight agency to conduct activities authorized by law, would include disclosure to private agencies working under government authorization. Oversight activities would include conducting or supervising: ▪ Audits ▪ Investigations ▪ Inspections ▪ Civil, criminal or administrative proceedings or actions ▪ Other activities necessary for appropriate oversight of the health care system, of government benefit programs for which health information is relevant to beneficiary eligibility, and of government regulatory programs for which health information is necessary for determining compliance with program standards.
Judicial and Administrative Proceedings pg. 59958	
	Covered entities can disclose PHI in a judicial or administrative proceeding if the request is made through or pursuant to a court order or an order by an administrative law judge specifically authorizing the disclosure of protected health information. A court order would not be needed if the PHI related to a party to the proceeding whose health condition is at issue (ex – Malpractice).

	Provisions for substance treatment or psychiatric counseling records, also consider preemptive state law.
Coroners and Medical Examiners pg. 59960	
	Covered entities can disclose PHI to a coroner or medical examiner to aid in identification of person or to determine the cause of death. Covered entities would have an obligation to verify the identity of the coroner or ME making the request before disclosure would be permitted.
Law Enforcement pg. 59960	
	Covered entities can disclose PHI to law enforcement officials conducting or supervising a law enforcement inquiry or proceeding authorized by law of the request for PHI is made ▪ Pursuant to a warrant, subpoena, or order issued by a judicial officer ▪ Pursuant to a grand jury subpoena ▪ Pursuant to an administrative subpoena or summons, civil investigation demand, or similar certification or written order (with some additional requirements) ▪ For limited identifying information ▪ By law enforcement officials requesting PHI about an individual who is or is suspected to be the victim of a crime, abuse, or other harm ▪ For conduct of intelligence activities conducted pursuant to the NSA ▪ To law enforcement officials when a covered entity believes in good faith that the disclosed PHI constitutes evidence of criminal conduct (with conditions) Note – related to Fraud and abuse investigations.
Governmental Health Data Systems pg. 59964	
Disclosure in PHI for inclusion in State or other governmental health data systems	Covered entities can disclose PHI for inclusion in State or other governmental health data systems when such disclosure is authorized by law for analysis in support of policy, planning, regulatory, and management functions. The recipient of the information must be a government agency or private entity acting on behalf of a government agency. Covered entities would have an obligation to verify the identity of the person requesting the information and the legal authority behind the request before the disclosure would be permitted.
Directory Information pg. 59965	
	Facility Patient Directory Informal (verbal) pt. permission required unless patient is unresponsive. If unresponsive information can be disclosed unless the covered entity has knowledge of past

patient instructions, also consider impact to patient related to disclosure.

Banking and Payment Purposes pg. 59966

PHI can be disclosed to financial institutions or entities acting for financial institutions for processing payments for health care and health care premiums.

Related to checks and credit card payment transactions sent to financial institutions

Permitted disclosure generally limited to:

- Name and address of the accountholder
- Name and address of the payer or provider
- Amount of the charge for health services
- Date services rendered
- Expiration date if applicable (credit card)
- Individual's Signature

Research pg. 59967

Covered entities permitted to use and disclose PHI for research provided that the covered entity receives documentation that the research protocol has been reviewed by the IRB or equivalent body and the board found that the research protocol meets specified criteria designed to protect the subject.

Research is defined as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge (From the Federal Policy for the Protection of Human Subjects aka "the Common rule")

Covered entities could disclose PHI under the following conditions:

- Privacy board review – this could be an IRB or equivalent privacy board regardless of sponsoring or funding sources
- Following criteria met
  1. The use or disclosure of PHI involves no more than minimal risk to the subjects
  2. The waiver or alteration will not adversely affect the rights and welfare of the subjects
  3. The research could not practicably be carried out without the waiver or alteration
  4. Whenever appropriate, the subjects will be provided with additional pertinent information after participation
  5. The research would be impracticable to conduct without the PHI
  6. The research project is of sufficient importance to outweigh the intrusion into the privacy of the individual whose information would be disclosed
  7. There is an adequate plan to protect the identifiers from improper use and disclosure
  8. There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers

  The first 4 criteria are from the Common Rule
- The IRB chairperson, or members designated to conduct such review, may carry out review of research that involves minimal risk and involves only individual's medical records.
- The clinical trails the research would fall in the Health Care Provider definition
- For purposes of research the protections of the privacy rule will end at the death of a subject.
- The covered entity would be required to verify the identity of the persons making request for PHI; IRB approval would constitute sufficient verification.

- When both the Common rule and HIPAA regs apply to research, both sets of regulations would need to be followed.
- If a covered entity obtains individual authorization for use or disclosure of PHI the requirements applicable to individual authorization for release of PHI would apply. The regulation would require more information to be given to individuals regarding who could see their information and how it would be used than the Common Rule requirements.

Note: Recipients of the PHI, the researchers, may not be HIPAA covered entities – ex a drug company.

Emergency Circumstances pg. 59971

Covered entities, consistent with applicable law and ethical conduct may disclose PHI based on a reasonable belief that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. (Ex.: person who is a threat to self or others)

Next-of-Kin pg. 59972

Verbal agreement from the individual prior to releasing info to the next of kin/SO. Where not possible to obtain permission information relevant to the involvement with care and consistent with good professional practice and ethics could be disclosed. Provider would be required to take reasonable steps to verify the identify of the next of kin.

Additional Uses and Disclosures Required by Other Law pg. 59973

Covered entities may use or disclose PHI if the use is not addressed elsewhere in §164.510, is required by other law, and meets relevant requirements of such law.

Application to Specialized Classes pg. 59973

Related to care of military personnel, DOD and DOS sponsored care, see §164.510(m)